



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/930,829

08/15/2001

Eric S. Gilbert

818002 (50239-00001)

1439

25231

7590

11/27/2006

MARSH, FISCHMANN & BREYFOGLE LLP  
3151 SOUTH VAUGHN WAY  
SUITE 411  
AURORA, CO 80014

EXAMINER

POPHAM, JEFFREY D

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 11/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/930,829

Applicant(s)

GILBERT ET AL.

Examiner

Jeffrey D. Popham

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 07 September 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 7,8,10-14,23-25 and 38-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 7,8,10-14,23-25 and 38-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- 1) ☐ Certified copies of the priority documents have been received.
  - 2) ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Remarks***

Claims 7, 8, 10-14, 23-25, and 38-54 are pending.

***Response to Arguments***

1. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

***Claim Objections***

2. Claims 10 and 11 are objected to because there is no claim 9 for which to be dependent from. Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 38-44, 46-48, 50, and 54 are rejected under 35 U.S.C. 102(b) as being anticipated by Halamka (Halamka et al., "Managing Care in an Integrated Delivery System via an Intranet", 1998, pp. 1-5).

Regarding Claim 38,

Halamka discloses a method for de-identification of records  
comprising:

Locating personal identification data fields in a plurality of records  
(page 2);

Parsing the personal identification data fields (page 2);

Deleting a first portion of the personal identification data fields  
(page 2); and

One-way encrypting a second portion of the personal identification  
data fields to generate one or more de-identified records (page 2).

Regarding Claim 54,

Claim 54 is a system claim that corresponds to method claim 38  
and is rejected for the same reasons.

Regarding Claim 39,

Halamka discloses selecting the second portion of the personal  
identification data fields for one-way encryption (page 2).

Regarding Claim 40,

Halamka discloses receiving the personal identification data fields  
with a client computer (page 2).

Regarding Claim 41,

Halamka discloses providing the one or more de-identified records  
to a server computer (pages 1-2).

Regarding Claim 42,

Halamka discloses formatting the personal identification data fields prior to one-way encrypting a second portion of the personal identification data fields (page 2).

Regarding Claim 43,

Halamka discloses using a mapping file to locate the personal identification data fields in the plurality of records (page 2).

Regarding Claim 44,

Halamka discloses determining a second portion of the personal identification data fields to be one-way encrypted in response to deleting the first portion of the personal identification data fields (page 2).

Regarding Claim 46,

Halamka discloses comparing the one or more de-identified records with one or more master records to determine linkage between the one or more de-identified records and the one or more master records (page 2).

Regarding Claim 47,

Halamka discloses a system for de-identifying records comprising:

A client computer having an interface for receiving records, wherein the client computer is adapted to locate personal identification data fields in the records, delete at least a portion of the personal identification data fields, and encrypt remaining personal identification data fields to generate encrypted personal identification data fields (pages 1-2).

Regarding Claim 48,

Halamka discloses a mapping file used to locate personal identification data fields in the records (pages 1-2).

Regarding Claim 50,

Halamka discloses that the encrypted personal identification data fields comprise one-way encryption with a first encryption algorithm to provide a first encryption result (pages 1-2).

4. Claims 47 and 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Morar (U.S. Patent 6,678,822).

Regarding Claim 47,

Morar discloses a system for de-identifying records comprising:

A client computer having an interface for receiving records, wherein the client computer is adapted to locate personal identification data fields in the records, delete at least a portion of the personal identification data fields, and encrypt remaining personal identification data fields to generate encrypted personal identification data fields (Column 8, line 55 to Column 9, line 4; Column 9, lines 42-53; and Column 11, lines 37-65).

Regarding Claim 48,

Morar discloses a mapping file used to locate personal identification data fields in the records (Column 5, line 57 to Column 6, line 4).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 38-46, 49-51, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Zubeldia (U.S. Patent 6,397,224).

Regarding Claim 38,

Morar discloses a method for de-identification of records comprising:

Locating personal identification data fields in a plurality of records (Column 8, line 55 to Column 9, line 4);

Parsing the personal identification data fields (Column 9, lines 4-14);

Deleting a first portion of the personal identification data fields (Column 9, lines 42-53); and

Encrypting a second portion of the personal identification data fields to generate one or more de-identified records (Column 11, lines 37-65);

But may not disclose that the encryption is one-way encryption.

Zubeldia, however, discloses one-way encrypting the selected data fields (Column 5, line 26 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention

to incorporate the anonymous linking system of Zubeldia into the data obscuring system of Morar as modified by Sweeney in order to allow the records to be de-identified, but still provide a way to link the de-identified records, so that research may be conducted on the data without releasing any identification information.

Regarding Claim 54,

Claim 54 is a system claim that corresponds to method claim 38 and is rejected for the same reasons.

Regarding Claim 39,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses selecting the second portion of the personal identification data fields for one-way encryption (Column 9, lines 42-53).

Regarding Claim 40,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses receiving the personal identification data fields with a client computer (Column 6, lines 34-52; and Column 8, lines 41-54).

Regarding Claim 41,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses providing the one or more de-identified records to a server computer (Column 9, line 54 to Column 10, line 4; and Column 12, lines 31-46).

Regarding Claim 42,



Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses formatting the personal identification data fields prior to encrypting a second portion of the personal identification data fields (Column 9, lines 4-14; and Column 11, lines 28-32); and Zubeldia discloses that the encryption is one-way encryption (Column 5, line 26 to Column 6, line 12).

Regarding Claim 43,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses using a mapping file to locate the personal identification data fields in the plurality of records (Column 5, line 57 to Column 6, line 4).

Regarding Claim 44,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Morar discloses determining a second portion of the personal identification data fields to be encrypted in response to deleting the first portion of the personal identification data fields (Column 9, lines 42-53; and Column 11, lines 37-65); and Zubeldia discloses that the encryption is one-way encryption (Column 5, line 26 to Column 6, line 12).

Regarding Claim 45,

Morar as modified by Zubeldia discloses the method of claim 44, in addition, Zubeldia discloses concatenating the personal identification data fields that are one-way encrypted with a seed value to provide seed value

identifiers (Column 5, line 26 to Column 6, line 12). Both SHA1 and MD5 concatenate the data with seed values.

Regarding Claim 46,

Morar as modified by Zubeldia discloses the method of claim 38, in addition, Zubeldia discloses comparing the one or more de-identified records with one or more master records to determine linkage between the one or more de-identified records and the one or more master records (Column 6, line 66 to Column 7, line 16; Column 7, line 64 to Column 8, line 6; and Column 8, line 62 to Column 9, line 4).

Regarding Claim 49,

Morar may not disclose that at least a portion of the personal identification data fields are encoded with a seed value to provide seed value identifiers.

Zubeldia, however, discloses that at least a portion of the personal identification data fields are encoded with a seed value to provide seed value identifiers (Column 5, line 26 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the anonymous linking system of Zubeldia into the data obscuring system of Morar as modified by Sweeney in order to allow the records to be de-identified, but still provide a way to link the de-identified records, so that research may be conducted on the data without releasing any identification information.

Regarding Claim 50,

Morar may not disclose that the encryption is one-way encryption.

Zubeldia, however, discloses one-way encrypting the selected data fields (Column 5, line 26 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the anonymous linking system of Zubeldia into the data obscuring system of Morar as modified by Sweeney in order to allow the records to be de-identified, but still provide a way to link the de-identified records, so that research may be conducted on the data without releasing any identification information.

Regarding Claim 51,

Morar as modified by Zubeldia discloses the system of claim 50, in addition, Zubeldia discloses that the encrypted personal identification data fields comprise one-way encryption with a second encryption algorithm to provide a second encryption result (Column 5, line 26 to Column 6, line 12).

6. Claims 7, 8, 10-12, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Sweeney (Sweeney, Latanya, "Guaranteeing Anonymity when Sharing Medical Data, the Datafly System", 1997, pp. 1-5, obtained from <http://lab.privacy.cs.cmu.edu/people/sweeney/>) and Zubeldia.

Regarding Claim 7,

Morar discloses a method for de-identification of records by and at a programmed client computer comprising:

Providing records to the programmed client computer (Column 6, lines 34-52; and Column 8, lines 41-54);

Locating personal identification data fields in each of the records (Column 8, line 55 to Column 9, line 4);

Parsing the personal identification data fields (Column 9, lines 4-14);

Formatting the personal identification data fields (Column 9, lines 4-14; and Column 11, lines 28-32);

Selecting at least a portion of the formatted personal identification data fields (Column 9, lines 42-53);

Determining if the selected the at least a portion of the formatted personal identification data fields is to be encoded (Column 9, lines 42-53);

Encoding the selected the at least a portion of the formatted personal identification data fields that is to be encoded (Column 9, lines 42-53);

Encrypting the encoded the at least a portion of the formatted personal identification data fields (Column 11, lines 37-65); and

A step of deleting personal identification data fields (Column 9, lines 42-53);

But may not disclose that the encryption is one-way encryption or the step of deleting any of the personal identification data fields that are not selected.

Sweeney, however, discloses parsing, formatting, selecting, determining if the selected personal identification data fields should be encoded, encoding the data fields to be encoded, and deleting any of the personal identification data fields that are not selected (Pages 3-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data anonymization technique of Sweeney into the data obscuring system of Morar in order to allow the system to encode and delete personal identification data fields based on a recipient's needs and anonymity level, so as to give the recipient as anonymous data as possible while still providing data that is useful.

Zubeldia, however, discloses one-way encrypting the selected data fields (Column 5, line 26 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the anonymous linking system of Zubeldia into the data obscuring system of Morar as modified by Sweeney in order to allow the records to be de-identified, but still provide a way to link the de-identified records, so that research may be conducted on the data without releasing any identification information.

Regarding Claim 23,

Claim 23 is a computer readable media claim that corresponds to method claim 7 and is rejected for the same reasons.

Regarding Claim 8,

Morar as modified by Sweeney and Zubeldia discloses the method of claim 7, in addition, Morar discloses obtaining a mapping file and locating personal identification data fields in each of the records using the mapping file (Column 5, line 57 to Column 6, line 4).

Regarding Claim 10,

Morar as modified by Sweeney and Zubeldia discloses the method of claim 7, in addition, Zubeldia discloses concatenating the encoded data with a seed value to provide seed value identifiers (Column 5, line 26 to Column 6, line 12).

Regarding Claim 11,

Morar as modified by Sweeney and Zubeldia discloses the method of claim 7, in addition, Morar discloses that the encoded the at least a portion of the formatted personal identification data fields are not concatenated with a seed value prior to the one-way encrypting (Column 8, line 55 to Column 9, line 53; and Column 11, lines 37-65).

Regarding Claim 12,

Morar as modified by Sweeney and Zubeldia discloses the method of claim 7, in addition, Zubeldia discloses one-way encrypting with a first encryption algorithm the encoded the at least a portion of the formatted

personal identification data fields selected to provide a first encryption result for each of the encoded the at least a portion of the formatted personal identification data fields selected (Column 5, line 26 to Column 6, line 12); and one-way encrypting with a second encryption algorithm the encoded the at least a portion of the formatted personal identification data fields selected to provide a second encryption result for each of the encoded the at least a portion of the formatted personal identification data fields selected (Column 5, line 26 to Column 6, line 12).

7. Claims 52 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Zubeldia, further in view of Schneier (Schneier, Bruce, "Applied Cryptography", Second Edition, 1996, pp. 193-193).

Regarding Claim 52,

Morar as modified by Zubeldia may not disclose concatenation of each of the first encryption result and the second encryption result to respectively provide binary string identifiers.

Schneier, however, discloses concatenation of each of the first encryption result and the second encryption result to respectively provide binary string identifiers (Pages 430-431, Length of One-Way Hash Functions section). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the method of increasing hash length from Schneier into the data obscuring system of

Morar as modified by Zubeldia in order to provide a more secure hash that cannot be broken as easily through birthday attacks, thus allowing a preventing a malicious entity from stealing other people's data.

Regarding Claim 53,

Morar as modified by Zubeldia and Schneier discloses the system of claim 52, in addition, Morar discloses that the binary strings are converted to alphanumeric strings to provide match codes (Column 7, lines 31-39).

8. Claims 13, 14, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Sweeney and Zubeldia, further in view of Schneier.

Regarding Claim 13,

Morar as modified by Sweeney and Zubeldia discloses the method of claim 12, in addition, Morar discloses converting binary strings to alphanumeric strings to provide match codes (Column 7, lines 31-39), but does not disclose concatenating at least a portion of each of the first encryption result and the second encryption result to respectively provide binary string identifiers.

Schneier, however, discloses concatenating at least a portion of each of the first encryption result and the second encryption result to respectively provide binary string identifiers (Pages 430-431, Length of One-Way Hash Functions section). It would have been obvious to one of



ordinary skill in the art at the time of applicant's invention to incorporate the method of increasing hash length from Schneier into the data obscuring system of Morar as modified by Sweeney and Zubeldia in order to provide a more secure hash that cannot be broken as easily through birthday attacks, thus allowing a preventing a malicious entity from stealing other people's data.

Regarding Claim 14,

Morar discloses a method for de-identification of records by a programmed client computer, comprising:

Monitoring a file directory (Column 6, lines 34-52; and Column 8, lines 41-54);

Detecting presence of a new file in the file directory (Column 6, lines 34-52; and Column 8, lines 41-54);

Obtaining a mapping file for the new file (Column 5, line 57 to Column 6, line 4);

Locating personal identification data fields in records in the new file using the mapping file (Column 8, line 55 to Column 9, line 4);

Parsing the personal identification data fields (Column 9, lines 4-14);

Formatting the personal identification data fields (Column 9, lines 4-14; and Column 11, lines 28-32);

Selecting at least a portion of the formatted personal identification data fields (Column 9, lines 42-53);

Determining if the selected the at least a portion of the personal identification data fields are to be encoded (Column 8, line 55 to Column 9, line 53; and Column 11, lines 37-65);

Encoding the selected the at least a portion of the personal identification data fields that are to be encoded (Column 8, line 55 to Column 9, line 53; and Column 11, lines 37-65);

Encrypting the data (Column 11, lines 37-65);

Converting binary strings to alphanumeric strings to provide match codes (Column 7, lines 31-39); and

A step of deleting personal identification data fields (Column 9, lines 42-53);

Wherein de-identified records comprising the match codes are created at a programmed client computer prior to transmission to a server computer (Column 9, line 54 to Column 10, line 4; and Column 12, lines 31-46);

But may not disclose that the encryption is one-way encryption or the step of deleting any of the personal identification data fields that are not selected, and concatenating at least a portion each of the first encryption result and the second encryption result to respectively provide binary string identifiers.

Sweeney, however, discloses parsing, formatting, selecting, determining if the selected personal identification data fields should be encoded, encoding the data fields to be encoded, and deleting any of the personal identification data fields that are not selected (Pages 3-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data anonymization technique of Sweeney into the data obscuring system of Morar in order to allow the system to encode and delete personal identification data fields based on a recipient's needs and anonymity level, so as to give the recipient as anonymous data as possible while still providing data that is useful.

Zubeldia, however, discloses concatenating the encoded the at least a portion of the personal identification data fields with a seed value to provide seed value identifiers; first one-way encrypting the seed value identifiers with a first encryption algorithm; second one-way encrypting the seed value identifiers with a second encryption algorithm (Column 5, line 26 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the anonymous linking system of Zubeldia into the data obscuring system of Morar as modified by Sweeney in order to allow the records to be de-identified, but still provide a way to link the de-identified records, so that research may be conducted on the data without releasing any identification information.

Schneier, however, discloses concatenating at least a portion each of the first encryption result and the second encryption result to respectively provide binary string identifiers (Pages 430-431, Length of One-Way Hash Functions section). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the method of increasing hash length from Schneier into the data obscuring system of Morar as modified by Sweeney and Zubeldia in order to provide a more secure hash that cannot be broken as easily through birthday attacks, thus allowing a preventing a malicious entity from stealing other people's data.

Regarding Claim 24,

Claim 24 is a computer readable media claim that corresponds to method claim 14 and is rejected for the same reasons.

Regarding Claim 25,

Morar as modified by Sweeney, Zubeldia, and Schneier discloses the computer readable media of claim 24, in addition, Morar discloses that the programmed client computer comprises a mapper program, a parser program, a formatting program, and an encoding program (Column 5, line 57 to Column 6, line 4; Column 8, line 55 to Column 9, line 53; and Column 11, lines 28-65).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham  
Examiner  
Art Unit 2137

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER